UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,516	05/24/2001	Nikhil M. Deshpande	P 279166 P11161	9874

27496 7590 06/24/2005

PILLSBURY WINTHROP SHAW PITTMAN LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,516	DESHPANDE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5, 7-10, 12-14, 17-25, 27-28, and 30* is/are pending in the application.

4a) Of the above claim(s) *6,11,15,16,26 and 29* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-10,12-14,17-25,27,28 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5, 7-10, 12-14, 17-25, 27-28, and 30 have been amended and are pending.

Applicant has cancelled claims 6, 11, 15-16, 26, and 29.

2. Claims 1-5, 7-10, 12-14, 17-25, 27-28, and 30 are rejected under 35 U.S.C. 103(a).

3. This is a Final rejection necessitate by new grounds of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 5, and 22-24 are rejected under 35 U.S.C. 103(a) as being obvious over Rautila (US 6,714,797).

As per claim 1:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising:

establishing a connection between the wireless device and the hotspot access point; **[COL.4, lines 45-48]**

providing information associated with the physical location of the hotspot access point to the wireless device; **[COL.5, lines 3-6]**

making a hand-off of the wireless device to a second hotspot access point; and **[COL.5, lines 20-21]**

providing narrowed information to the wireless device associated with a physical location of the second hotspot access **[COL.8, lines 27-31]** point based upon the direction of travel of the wireless device. **[COL.4, lines 48-59 and COL.5, lines 58-60]**

Rautila discusses each hotspot network has at least one hotspot device (col.4, lines 48-49) and be able to determine the nearest locations of the hotspot network by using the user's starting location (col.8, lines 30-31).

Therefore, it is obvious to an ordinary skill in the art at the time of the invention was made for Rautila to include a second hotpot location wherein directing the user to the location where the product can be downloaded (col.5, lines 58-60) by transmitting the nearest locations within the hotspot network and having a list of hotspot locations to the user (col.6, lines 32-34).

As per claim 2:

Rautila discusses a method of claim 1, further comprising:

identifying the hotspot access point with which the wireless device is connected; and **[COL.6, lines 47-49 and COL.8, lines 27-31]**

determining information associated with the physical location of the access point using the identification of the hotspot access point in a look-up

database. **[COL.6, lines 32-34 and COL.8, lines 60-61]**

As per claim 5: See COL.4, lines 15-40; discussing the access point is a wireless LAN access point device.

As per claim 6: Cancelled

As per claim 22:

Rautila discloses computer program product including computer program code, the computer program code having instructions, which when executed cause a computer to:

establish a connection between the wireless device and the hotspot access point; **[COL.4, lines 45-50 and COL.5, lines 3-6]**

provide information associated with the physical location of the hotspot access point to the wireless device; **[COL.7, lines 23-35 and COL.8, lines 27-34]**

making a hand-off of the wireless device to a second hotspot access point; and **[COL.5, lines 20-21]**

providing the narrowed information associated with a physical location of the second hotspot access point based on the direction of travel of the wireless device. **[COL.5, lines 58-60 and COL.8, lines 27-31]**

Rautila discusses each hotspot network has at least one hotspot device (col.4, lines 48-49) and be able to determine the nearest locations of the hotspot network by using the user's starting location (col.8, lines 30-31).

Therefore, it is obvious to an ordinary skill in the art at the time of the invention was made for Rautila to include a second hotpot location wherein directing the user to the location where the product can be downloaded (col.5, lines 58-60) by transmitting the nearest locations within the hotspot network and having a list of hotspot locations to the user (col.6, lines 32-34).

As per claim 23:

Rautila discusses computer program product of claim 22, having instructions, which when executed cause a computer to:

identify the hotspot access point with which the wireless device is connected; and **[COL.6, lines 47-49 and COL.8, lines 27-31]**

determine information associated with the physical location of the access point using the identification of the hotspot access point in a look-up database. **[COL.6, lines 32-34 and COL.8, lines 60-61]**

As per claim 24: See COL.6, lines 33-53 and COL.7, lines 11-12; discussing to provide security for the location-based services according to a mode of a plurality of modes of security, the mode of security having associated therewith routing identification information.

As per claim 26: Cancelled

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 7-8, 10, 12-14, 17, 19-21, 27, and 30are rejected under 35 U.S.C. 103(a) as being unpatentable over Rautila (US 6,714,797) and in further view of Spies, et al. (US 6,230,269).

As per claim 3:

Rautila discloses providing security for the location-based services according to a mode of security of plurality of security modes, the mode having associated therewith routing identification information (COL.6, lines 33-38 and 47-53 and COL.8, lines 27-34). Rautila discusses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38) that identifies a electric shop and product(col.5, lines 50-60) .

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content

provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Hence, it is obvious to an ordinary skill in the art at the time of the invention was made to include routing identification such as unique order number with user/device identification information of Spies within the logon process of Rautila because this information where the product is located and where the user is authorized to download according to the particular the hotspot network location.

As per claim 7:

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies

the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location.

As per claim 8:

Rautila discloses method of securing services provided through a hotspot access point, comprising:

establishing a connection between a wireless device and the hotspot access point; **[COL.4, lines 45-50 and COL.5, lines 3-6]**

determining user/device identification information associated with the wireless device; **[COL.5, lines 57- COL.6, line 2]**

identifying mode of security from a plurality of security modes for the services using the user/device identification information, the identified mode of security having associated therewith routing identification information; and **[COL.6, lines 33-53]**

providing the services **[COL.7, lines 11-12]** according to the identified mode of security using the routing identification information through the hotspot access point to the wireless device. **[COL.7, lines 23-35 and COL.8, lines 27-34]**

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60), and routing identification such as unique order number identifies a electric shop (col.5, lines 50-60) and the product the user is authorized to download at the particular location (col.6, lines 37-53). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location and products according to the user ID.

As per claim 10:

See COL.4, lines 40; discusses the plurality of security of modes includes private, public and personal mode.

As per claim 11: Cancelled

As per claim 12:

A method of billing services provided through a hotspot access point, comprising:

establishing a connection between a wireless device and the hotspot access point; **[COL.4, lines 45-48]**

determining user/device identification information associated with the wireless device; and **[COL.5, lines 57- COL.6, line 2]**

billing usage of the services through the access point by the wireless device according to a mode of billing identified by the user/device identification information, **[COL.6, lines 9-19]**

wherein the mode of billing business, public and personal modes, wherein the private mode includes billing a business entity other than an actual user of the wireless device or a service provider associated with the

wireless device or the actual user of the wireless device, the public mode includes billing the actual user of the wireless device, and the personal mode includes billing the service provider associated with the wireless device.

[COL.8, lines 16-22]

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious to an ordinary skill in the art at the time of the invention was made the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location.

As per claim 13:

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location.

As per claim 14: See COL.6, lines 33-38 and 47-53 and COL.8, lines 27-34; discusses providing information associated with the physical location of the hotspot access point to the wireless device.

As per claim 15: Cancelled

As per claim 16: Cancelled

As per claim 17:

Rautila discloses a system of providing location-based services to a wireless device using a

hotspot access point, comprising:

the hotspot access point to establish a connection between the wireless device and a hotspot access point network; **[COL.4, lines 45-48]**

location-based services server to provide information associated with the physical location of the hotspot access point to the wireless device; and **[COL.7, lines 28-38]**

an authorization server to provide security for the location-based services **[COL.5, lines 57- COL.6, line 2]** according to a mode of security of a plurality of security modes **[COL.7, lines 11-12]**, the mode of security having associated therewith routing identification information. **[COL.6, lines 33-53]**

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38) that identifies a electric shop and product(col.5, lines 50-60) .

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Hence, it is obvious to an ordinary skill in the art at the time of the invention was made to include routing identification such as unique order number with user/device identification information of Spies within the logon process of Rautila because this information where the product is located and where the user is authorized to download according to the particular the hotspot network location.

As per claim 19: See COL.4, lines 15-40; discussing the access point is a wireless LAN access point device.

As per claim 20:

Rautila discusses the system of claim 15, wherein the location-based services server:

makes a hand-off of the wireless device to a second hotspot access point; **[COL.5, lines 20-21]**

narrows the information provided to the wireless device with respect to the physical location of the second hotspot access point based upon the direction of travel of the wireless device; and **[COL.4, lines 48-59 and COL.6, lines 32-34]**

provides the narrowed information associated with the physical location of the second hotspot access point to the wireless device. **[COL.5, lines 58-60 and COL.8, lines 27-31]**

Rautila discusses each hotspot network has at least one hotspot device (col.4, lines 48-49) and be able to determine the nearest locations of the hotspot network by using the user's starting location (col.8, lines 30-31).

Therefore, it is obvious to an ordinary skill in the art at the time of the invention was made for Rautila to include a second hotpot location wherein directing the user to the location where the product can be downloaded (col.5, lines 58-60) by transmitting the nearest locations within the hotspot network and having a list of hotspot locations to the user (col.6, lines 32-34).

As per claim 21:

Rautila discloses providing security for the location-based services according to a mode of security of plurality of security modes, the mode having associated therewith routing identification information (COL.6, lines 33-38 and 47-53 and COL.8, lines 27-34). Rautila discusses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38) that identifies a electric shop and product(col.5, lines 50-60) .

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location.

As per claim 27:

Rautila discloses computer program product including computer program code having instructions, which when executed cause a computer to:

establish a connection between a wireless device and the hotspot access point; **[COL.4, lines 45-50 and COL.5, lines 3-6]**

determine user/device identification information associated with the wireless device; **[COL.5, lines 10-21]**

identify a mode of security of a plurality of modes of security **[COL.7, lines 11-12]** for the services using the user/device identification information, the mode of security having associated therewith routing identification information; and **[COL.6, lines 33-53]**

providing the services according to the mode of security using the routing identification information through the hotspot access point to the wireless device. **[COL.7, lines 23-35 and COL.8, lines 27-34]**

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60), and routing identification such as unique order number identifies a electric shop (col.5, lines 50-60) and the product the user is authorized to

download at the particular location (col.6, lines 37-53). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location and products according to the user ID.

As per claim 29: Cancelled

As per claim 30:

Rautila discloses computer program product including computer program code, the computer program code having instructions, which when executed cause a computer to:

establishing a connection between a wireless device and the hotspot access point; **[COL.4, lines 45-48]**

determining user/device identification information associated with the wireless device; and **[COL.5, lines 57- COL.6, line 2]**

billing usage of the services through the access point by the wireless device according to a mode of billing identified by the user/device identification information, **[COL.6, lines 9-19]**

wherein the mode of billing business, public and personal modes, wherein the private mode includes billing a business entity other than an actual user of the wireless device or a service provider associated with the wireless device or the actual user of the wireless device, the public mode includes billing the actual user of the wireless device, and the personal mode includes billing the service provider associated with the wireless device. **[COL.8, lines 16-22]**

Rautila discloses directing a user to a hotspot location where the product to be downloaded at the order/location module and gaining access by a logon process (col.6, lines 1-2) and giving a unique order number to the user (col.6, lines 37-38). Hence, it is obvious the logon process may include some kind of user/device identification information to identify the user to gain access to the hotspot and to the vendors/products available on the hotspot network (col.7, lines 10-60). However, Rautila fails to explain further the details of the logon process.

Spies, et al. teaches an authentication system for a distributed network having multiple clients and a server that enables a user to log on and verifies

the identity of the user (col.1, lines 13-16) wherein the server can be a content provider, web site, or an Internet service providers (col.3, lines 60-65) and the client can be a computer or a wireless device such as a laptop. Spies discusses the log on process includes user ID or user identification information which may consist of any of the following user name, PIN, serial number, etc. (col.4, lines 37-45).

Therefore it would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the user identification information of Spies with the logon process of Rautila because the user ID is the security feature that identifies the user to gain access to the hotspot network location.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4, 9, 18, 25, and 28, are rejected under 35 U.S.C. 103(a) as being unpatentable over Rautila (US 6,714,797), and further in view of Microsoft Computer Dictionary, 5th Edition.

As per claim 4:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising establishing a connection between the wireless device and the hotspot access point **[COL.4, lines 45-50 and COL.5, lines 3-6]** and providing information associated with the physical location of the hotspot access point to the wireless device **[COL.5, lines 20-21 and COL.8, lines 27-31]**. However, Rautila fails to include the routing identification information is an IP address.

According to the Microsoft Computer Dictionary, IP address identifies a host (computer). It would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the teaching of the IP address of the Microsoft Dictionary with Raulita as a routing identification because the address uniquely identifies a computer connected to the Internet to other Internet hosts **[pg.287]**

As per claim 9:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising establishing a connection between the wireless device and the hotspot access point **[COL.4, lines 45-50 and COL.5, lines 3-6]** and providing information associated with the physical location of the hotspot access point to the wireless device **[COL.5, lines 20-21 and COL.8, lines 27-31]**. However, Rautila fails to include the routing identification information is an IP address.

According to the Microsoft Computer Dictionary, IP address identifies a host (computer). It would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the teaching of the IP address of the Microsoft Dictionary with Rautila as a routing identification because the address uniquely identifies a computer connected to the Internet to other Internet hosts **[pg.287]**

As per claim 18:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising establishing a connection between the wireless device and the hotspot access point **[COL.4, lines 45-50 and COL.5, lines 3-6]** and providing information associated with the physical location of the hotspot access point to the wireless device **[COL.5, lines 20-21 and COL.8, lines 27-31]**. However, Rautila fails to include the routing identification information is an IP address.

According to the Microsoft Computer Dictionary, IP address identifies a host (computer). It would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the teaching of the IP address of the Microsoft Dictionary with Raulita as a routing identification because the address uniquely identifies a computer connected to the Internet to other Internet hosts **[pg.287]**

As per claim 25:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising establishing a connection between the wireless device and the hotspot access point **[COL.4, lines 45-50 and COL.5, lines 3-6]** and providing information associated with the physical location of the hotspot access point to the wireless device **[COL.5, lines 20-21 and COL.8, lines 27-31]**. However, Rautila fails to include the routing identification information is an IP address.

According to the Microsoft Computer Dictionary, IP address identifies a host (computer). It would have been obvious to combine the teaching of the IP address of the Microsoft Dictionary with Raulita as a routing identification because the address uniquely identifies a computer connected to the Internet to other Internet hosts **[pg.287]**

As per claim 28:

Rautila discloses a method of providing location-based services to a wireless device using a hotspot access point, comprising establishing a connection between the wireless device and the hotspot access point **[COL.4, lines 45-50 and COL.5, lines 3-6]** and providing information associated with the physical location of the hotspot access point to the wireless device **[COL.5, lines 20-21 and COL.8, lines 27-31]**. However, Rautila fails to include the routing identification information is an IP address.

According to the Microsoft Computer Dictionary, IP address identifies a host (computer). It would have been obvious to an ordinary skill in the art at the time of the invention was made to combine the teaching of the IP address of the Microsoft Dictionary with Raulita as a routing identification because the address uniquely identifies a computer connected to the Internet to other Internet hosts **[pg.287]**

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100